UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/058,442	01/28/2002	Robert J. Donaghey	BBNT-P02-369	5927

28120 7590 07/27/2006

FISH & NEAVE IP GROUP
ROPES & GRAY LLP
ONE INTERNATIONAL PLACE
BOSTON, MA 02110-2624

EXAMINER	
WILSON, ROBERT W	

ART UNIT	PAPER NUMBER
2616	

DATE MAILED: 07/27/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/058,442	DONAGHEY, ROBERT J.	
	Examiner	Art Unit	
	Robert W. Wilson	2616	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 June 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,9-12,14-17,19-28,30-33,36-43 and 46-56* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4,10-12,14,20-27,30-33,36,37,41,42 and 46-56* is/are rejected.

7)☒ Claim(s) *5-7,9,15-17,19,28,38-40 and 43* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 1/28/02, 10/27/05, & 1/25/03
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Claim Objections

1. Claims 5-7, 9, 15-17, 19, 28-31, & 38-40 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 46-56 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Referring to claims 46-51, 53, & 55; the applicant claims describe a first filter in which no filtering or unfiltering is performed on a current group of packets after subsequently processing previously received. What is meant by " a first filter perform unfiltering or no filtering. What is meant by "receiving a group of packets from a first user subsequent to the application of the first filtering technique comprises receiving an unfiltered group of packets subsequent to the first filtering technique being applied to the previously received group of packets" as claimed in claim 46. The concept of this comment applies to claims 47-51, 53, & 55 respectively. In essence the applicant has defined a first filter that unfilters or does not filter.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-2, 4, 10-12, 14, 20-24, 46, & 48 are rejected under 35 U.S.C. 102(e) as being anticipated by Strayer (Patent Pub: US2003/0097439).

Referring to claim 1, Strayer discloses a method for modeling a behavior or normal users in a network per Figures 6 & 7A in response to an application of first filtering (Traffic auditor 130) and: first filtering technique is provided by Traffic auditors 130 that sample packets of the one or more flows per step 705 in Figure 7A and Para [106] lines 3-6 comprising:

Receiving a group of packets form a first user subsequent to the application of the first filtering technique (receiving packets and storing them to determine behavior of the first user based upon a group of packets per step 710 in Figure 7A and Para 0106 lines 9-11)

Associating at least one feature with each packet in the group of packets (The reference discloses in Para 0106 of Page 8 that the traffic analysis maybe performed based upon Figure 6. Step 615 of Figure 6 discloses that classification of traffic flows or groups of packets is performed based upon feature sets or at least one feature)

Creating at least one model reflecting the behavior of the first user on the feature sets associated with the traffic flow or group of packets (Step 725 in Figure 7A and Para 0108 lines 1-3 and Step 615 of Figure 6.)

In Addition Strayer discloses:

Regarding claim 2, wherein at least one includes Hidden Markov Models (Para 103 lines 5-8)

Regarding claim 4, wherein the at least one feature includes at least characteristics of packet headers (Para 0111 lines 20-23)

Regarding claim 46, wherein receiving a group of packets from a first user subsequent to the application of the first filtering technique comprises receiving an unfiltered group of packets subsequent to the first filtering technique being applied to a previously received group of packets (The applicant describes a filter that does not filter or receiving packets and storing them to determine behavior of the first user based upon a group of packets current packets and subsequent packets per step 710 in Figure 7A and Para 0106 lines 9-11)

Regarding claim 10, wherein the receiving includes: receiving a stream of packets from a plurality of users, identifying the packets in the stream to obtain identified first user packets, and grouping said identified first user packets (plurality of nodes and traffic auditors that identify packets per Figure 1 and per Para 0023 lines 3-4 and Para 0024 lines 1-3 respectively.

Referring to claim 11, Strayer discloses a method for modeling a behavior or normal users in a network per Figures 6 & 7A comprising:

a memory configured to store instructions (memory 310 per Figure 3);

a processor configured to execute the instructions (Processor 305 in Figure 3); to filter packets in the network using a first filtering technique (Traffic Auditors 130 per Figure 3 that samples and examines the packets);

receive a group of packets from a first user after filtering (receiving packet and storing them to determine behaviors per Step 710 in figure 7A and per Para 0106 lines 9-11)

Associate at least one feature with each packet in the group of packets (The reference discloses in Para 0106 of Page 8 that the traffic analysis maybe performed based upon Figure 6. Step 615 of Figure 6 discloses that classification of traffic flows or groups of packets is performed based upon feature sets or at least one feature)

Create at least one model reflecting the behavior of the first user on the feature sets associated with the traffic flow or group of packets (Step 725 in Figure 7A and Para 0108 lines 1-3 and Step 615 of Figure 6.)

In Addition Strayer discloses:

Regarding claim 12, wherein at least one includes Hidden Markov Models (Para 103 lines 5-8)

Regarding claim 14, wherein the at least one feature includes at least characteristics of packet headers (Para 0111 lines 20-23)

Regarding claim 20, wherein the receiving includes: receiving a stream of packets from a plurality of users, identifying the packets in the stream to obtain identified first user packets, and grouping said identified first user packets (plurality of nodes and traffic auditors that identify packets per Figure 1 and per Para 0023 lines 3-4 and Para 0024 lines 1-3 respectively.

Regarding claim 47, wherein the group of packets comprises an unfiltered group of packets received subsequent to the first filtering technique being applied to a previously received group of packets (The applicant describes a filter that does not filter or receiving a group of packets and storing them to determine behavior of the first user based upon a group of packets current packets and subsequent group of packets per step 710 in Figure 7A and Para 0106 lines 9-11)

Referring to claim 21, Strayer discloses a computer-readable medium containing instructions (Memory 310 per Figure 3) for controlling at least one processor (Processor 305 in Figure 3) to perform a method for modeling a behavior of users in a network in response to an application of a first filtering technique (step 710 in Figure 7A and Para 0106 lines 9-11)

Receiving a group of packets from a first user subsequent to the application of the first filtering technique (receiving packets and storing them to determine behavior of the first user based upon a group of packets per step 710 in Figure 7A and Para 0106 lines 9-11)

Associating at least one feature with each packet in the received packets (The reference discloses in Para 0106 of Page 8 that the traffic analysis maybe performed based upon Figure 6. Step 615 of Figure 6 discloses that classification of traffic flows or groups of packets is performed based upon feature sets or at least one feature)

Creating at least one model reflecting the behavior of the first user on the feature sets associated with the traffic flow or group of packets (Step 725 in Figure 7A and Para 0108 lines 1-3 and Step 615 of Figure 6.)

In Addition Strayer discloses:

Regarding claim 22, wherein at least one includes Hidden Markov Models (Para 103 lines 5-8)

Regarding claim 23, wherein the at least one feature includes at least characteristics of packet headers (Para 0111 lines 20-23).

Regarding claim 24, receiving a stream of packets from a plurality of users (Steps 710 & 715 per Figure 7A) and grouping packets associated with the first user (615 & 620 per Figure 6 and Unique ID from sender per Para 0042 on Pg 4.

Regarding claim 48, wherein the received packets comprise unfiltered packet received subsequent to the application of the first filtering technique to a group of previously received packets (The applicant describes a filter that does not filter or receiving a group of packets and storing them to determine behavior of the first user based upon a group of packets current packets and subsequent group of packets per step 710 in Figure 7A and Para 0106 lines 9-11)

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 23-27, 30-33, 36-37, 41-42, & 49-56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Strayer (Patent Pub: US2003/0097439).

Referring to claim 25 & 32, Strayers discloses a method and a system for identifying anomalies in network data streams and denying an attack and applying filtering technique per Figures 6 and 7A comprising: means for receiving , subsequent to a filtering technique being applied, a stream of packets (receiving packets and storing them to determine behavior Step 710 in Figure 7A or Para 0106 lines 9-11);

Means for partitioning the packets into group corresponding to a plurality of packets (receiving packets and storing them in groups in memory to determine behavior per Step 710 in Figure 7A or Para 0106 lines 9-11); means for classifying each group of packets as a normal group or attack group using at least one model, each model reflecting a normal response to an application of the filtering technique (using the developed mode one or more flows can be analyzed to determine deviations from the normal behavior per Step 725 in figure 7A and per Para 0108 lines 6-9.

Means for filtering out expected or normal traffic per Step 715 in Figure 7A.

The reference teaches: Filtering out expected traffic from the accumulate traffic per Step 715 and investigating Anomalous or Suspicious Traffic per Step 720 in Figure 7A. Filtering out expected

traffic from the accumulate traffic per Step 715 and investigating Anomalous or Suspicious Traffic per Step 720 in Figure 7A. When one filters out expected traffic from the accumulate traffic per Step 715 and investigates Anomalous or Suspicious Traffic per Step 720 in Figure 7A this method results in separation of expected traffic or means for separation of normal traffic Determining accumulated traffic minus expected traffic is attack group traffic or means for filtering groups of packets classified as attack groups using the first filtering technique. Strayer does not expressly call for allowing groups of packets classified as normal groups to pass on toward their destinations

Strayer teaches: Filtering out expected traffic from the accumulate traffic per Step 715 and investigating Anomalous or Suspicious Traffic per Step 720 in Figure 7A. Filtering out expected traffic from the accumulate traffic per Step 715 and investigating Anomalous or Suspicious Traffic per Step 720 in Figure 7A and when one filters out expected traffic from the accumulate traffic per Step 715 and investigates Anomalous or Suspicious Traffic per Step 720 in Figure 7A this method results in separation of expected traffic or means for separation of normal traffic It would have been obvious to one of ordinary skill in the art at the time of the invention that the normal traffic would have been allowed to travel to their destination in order for the invention to work.

In Addition Strayer teaches:

Regarding claim 26, identifying the packets in the stream to obtain identified first user packets, and grouping said identified first user packets (plurality of nodes and traffic auditors that identify packets per Figure 1 and per Para 0023 lines 3-4 and Para 0024 lines 1-3 respectively) associated each packet with a feature (Figure 6)

Regarding claim 27, wherein the at least one feature includes at least characteristics of packet headers (Para 0111 lines 20-23)

Regarding claim 30, wherein at least one includes Hidden Markov Models (Para 103 lines 5-8)

Regarding claim 31, wherein at least one model relates to filtering technique (Step 715 and Step 725 per Figure 7A)

Regarding claim 49 & 51, wherein receiving a stream of packets comprises receiving an unfiltered stream of packets subsequent to the first filtering technique being applied to a previously received stream of packets (Step 715 per Figure 7A shows no filtering or unfiltering of expected traffic through a first filter)

Referring to claim 50, Strayer teaches the method of claim 32 and determining expected traffic or normal groups. Strayer does not expressly call for: normal groups to pass on to their destination.

It would have been obvious to one of ordinary skill in the art at the time of the invention that the expected traffic would pass on to their destination in order for the invention to work.

Regarding claims 52, the unfiltered packets are the expected traffic or normal packets per Step 715 per Figure 7A.

Referring to claim 33, Strayers discloses a system for identifying normal traffic during a network attack per Figures 6 and 7A comprising:

Comprising a memory (memory 310 in Figure 3), each model reflecting a normal response to an application of a filtering technique (Using the developed model one or more flows can be

analyzed to determine deviations from normal behavior therefore normal and abnormal behavior can be determined per Step 725 in Figure 7A. Para 0108 lines 6-9)

A processor (Processor 305 in Figure 3)

Comprising receive a stream of packets subsequent to a first filtering technique being applied (receiving packets and storing them to determine behavior per Step 710 in Figure 7A or Para 0106 lines 9-11)

Partitioning a stream into strands-groups, each strand corresponding to a plurality of packets (Para 0104)

Classify each strand an at least one of a normal strand and an attack strand using at least one of the plurality of models (using the developed model one or more flows can be analyzed to determine deviations from normal behavior per Step 725 in Figure 7A or Para 0108 lines 6-9

The reference teaches: Filtering out expected traffic from the accumulate traffic per Step 715 and investigating Anomalous or Suspicious Traffic per Step 720 in Figure 7A. Filtering out expected traffic from the accumulate traffic per Step 715 and investigating Anomalous or Suspicious Traffic per Step 720 in Figure 7A. When one filters out expected traffic from the accumulate traffic per Step 715 and investigates Anomalous or Suspicious Traffic per Step 720 in Figure 7A this method results in separation of expected traffic or traffic classified as normal strands.)

Determining accumulated traffic minus expected traffic is attack group traffic or filter strands classified as attack strands using the first filtering technique

Strayer does not expressly allow strands classified as normal strands to pass on toward their destinations

Strayer teaches: Filtering out expected traffic from the accumulate traffic per Step 715 and investigating Anomalous or Suspicious Traffic per Step 720 in Figure 7A. Filtering out expected traffic from the accumulate traffic per Step 715 and investigating Anomalous or Suspicious Traffic per Step 720 in Figure 7A and when one filters out expected traffic from the accumulate traffic per Step 715 and investigates Anomalous or Suspicious Traffic per Step 720 in Figure 7A this method result in separation of expected traffic or separation of normal strands

It would have been obvious to one of ordinary skill in the art at the time of the invention that the normal traffic or normal strands would have been allowed to travel to their destination in order for the invention to work.

In Addition Strayer discloses:

Regarding claim 36, wherein the partitioning processor groups packets in the stream based on a source of the packets (Step 615 & 620 per Figure 6 determine flows or streams based upon feature and geo-location associated with the sender or source per Para 0042 Pg 4)

Regarding claim 37, wherein the processor is further configured to associate at least one of a plurality of previously defined features with each packet in the stream (Step 700 Figure 7A. Traceback Manger may request signatures-features-of packets per Para 0109 lines 10-12)

Regarding claim 53, wherein receiving a stream of packets comprises receiving an unfiltered stream of packets subsequent to the first filtering technique being applied to a previously received stream of packets (Step 715 per Figure 7A shows no filtering or unfiltering of expected traffic through a first filter)

Regarding claims 54, the unfiltered strands are the expected traffic or normal strands per Step 715 per Figure 7A.

Referring to claim 41, Strayer discloses a computer-readable medium containing instructions (memory 310 per Figure 3) for controlling at least one processor (Processor 305 per Figure 3) to perform a method for identifying normal traffic during a network attack comprising:
Receiving, subsequent to an application of a first filtering technique a stream of packets and grouping packets in the stream based on at least a source or packets (receiving packets and storing them in groups and determine packets behavior Step 710 in Figure 7A or per Para 0106 lines 9-11) and identifying, through the use of Hidden Markov Models each packet group as a normal group or attack group (using the developed model one or more flows can be analyzed to determine deviations from normal behavior-normal and abnormal behavior packets can be identified per Step 725 in Figure 7A and per Para 0108 lines 6-9), the HMMs representing normal response to the application of the first filtering technique.
The reference teaches: Filtering out expected traffic from the accumulate traffic per Step 715 and investigating Anomalous or Suspicious Traffic per Step 720 in Figure 7A. Filtering out expected traffic from the accumulate traffic per Step 715 and investigating Anomalous or Suspicious Traffic per Step 720 in Figure 7A. When one filters out expected traffic from the accumulate traffic per Step 715 and investigates Anomalous or Suspicious Traffic per Step 720 in Figure 7A this method results in separation of expected traffic or traffic classified as normal strands.)
Determining accumulated traffic minus expected traffic is attack group traffic or filtering packet groups classified as attack groups using the first filtering technique

Strayer does not expressly call for: allow strands classified as normal strands to pass on toward their destinations

Strayer teaches: Filtering out expected traffic from the accumulate traffic per Step 715 and investigating Anomalous or Suspicious Traffic per Step 720 in Figure 7A. Filtering out expected traffic from the accumulate traffic per Step 715 and investigating Anomalous or Suspicious Traffic per Step 720 in Figure 7A and when one filters out expected traffic from the accumulate traffic per Step 715 and investigates Anomalous or Suspicious Traffic per Step 720 in Figure 7A this method result in separation of expected traffic or separation of normal strands

It would have been obvious to one of ordinary skill in the art at the time of the invention that the normal traffic or normal strands would have been allowed to travel to their destination in order for the invention to work.

In Addition Strayer discloses:

Regarding claim 42, further comprising associating at least one feature with each packet in the stream of packets per Step 750 in figure 7A. Traceback Manager may request signatures-features of packets per Para 0109 lines 10-12)

In Addition Strayer discloses:

Regarding claim 55, wherein receiving a stream of packets comprises receiving an unfiltered stream of packets subsequent to the first filtering technique being applied to a previously received stream of packets (Step 715 per Figure 7A shows no filtering or unfiltering of expected traffic through a first filter)

Referring to claim 56, Strayer teaches the computer readable medium of claim 55 and determining expected traffic or normal groups.

Strayer does not expressly call for: normal groups to pass on to their destination.

It would have been obvious to one of ordinary skill in the art at the time of the invention that the expected traffic would pass on to their destination in order for the invention to work.

Response to Amendment

11. Applicant's arguments filed 6/19/06 have been fully considered but they are not persuasive.

The applicant incorporated the objected to dependent claims; however, upon further consideration the examiner has determined the amended independent claim can still be rejected by the cited prior art. Please refer to the above rejection for details.

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Robert W. Wilson whose telephone number is 571/272-3075. The examiner can normally be reached on M-F (8:00-4:30).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Doris To can be reached on 571/272-7629. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Robert W. Wilson

Robert W Wilson
Examiner
Art Unit 2616

RWW
7/20/06

DORIS H. TO
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600